

(2) Whether the cost of collecting the information from the individual is unreasonable when compared with the cost of collecting it from a third party;

(3) Whether there is a risk that information requested from the third parties, if inaccurate, could result in an adverse determination to the individual concerned;

(4) Whether the information, if supplied by the individual, would have to be verified by a third party; or

(5) Whether provisions can be made for verification by the individual of information collected from third parties.

(e) Employees whose duties require handling of records subject to the Act shall, at all times, take care to protect the integrity, security and confidentiality of these records.

(f) No employee of the section may alter or destroy a record subject to the Act unless (1) such alteration or destruction is properly undertaken in the course of the employee's regular duties or (2) such alteration or destruction is required by a decision of the Commissioner or the decision of a court of competent jurisdiction.

§ 1101.4 Reports on new systems of records; computer matching programs.

(a) Before establishing any new systems of records, or making any significant change in a system of records, the Section shall provide adequate advance notice to:

(1) The Committee on Government Operations of the House of Representatives;

(2) The Committee on Governmental Affairs of the Senate; and

(3) The Office of Management and Budget.

(b) Before participating in any computerized information "matching program," as that term is defined by 5 U.S.C. 552a(a)(8) the Section will comply with the provisions of 5 U.S.C. 552a(o), and will provide adequate advance notice as described in § 1101.4(a) above.

§ 1101.5 Security, confidentiality and protection of records.

(a) The Act requires that records subject to the Act be maintained with appropriate administrative, technical and

physical safeguards to ensure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience or unfairness to any individual on whom information is maintained.

(b) When maintained in manual form (typed, printed, handwritten, etc.) records shall be maintained, at a minimum, subject to the following safeguards, or safeguards affording comparable protection:

(1) Areas in which the records are maintained or regularly used shall be posted with an appropriate warning stating that access to the records is limited to authorized persons. The warning shall also summarize the requirements of § 1101.3 and state that the Act contains a criminal penalty for the unauthorized disclosure of records to which it applies.

(2) During working hours: (i) The area in which the records are maintained or regularly used shall be occupied by authorized personnel or (ii) access to the records shall be restricted by their storage in locked metal file cabinets or a locked room.

(3) During non-working hours, access to the records shall be restricted by their storage in locked metal file cabinets or a locked room.

(4) Where a locked room is the method of security provided for a system, that security shall be supplemented by: (i) Providing lockable file cabinets or containers for the records or (ii) changing the lock or locks for the room so that they may not be opened with a master key. For purposes of this paragraph, a master key is a key which may be used to open rooms other than the room containing records subject to the Act, unless those rooms are utilized by officials or employees authorized to have access to the records subject to the Act.

(5) Personnel handling personal information during routine use will ensure that the information is properly controlled to prevent unintentional or unauthorized disclosure. Such information will be used, held, or stored only